Errata/Typos for “Introduction to Modern Cryptography, third edition”

(Last updated April 7, 2022)

Note: negative line numbers correspond to counting from the bottom of the page.

- page 252, line -2 of Construction 7.6: $z_i^*$ should be $y_i^*$.

- page 362, Exercise 9.24: For this problem, assume that the twisted Edwards representation uses quadratic residue $a$ and quadratic non-residue $d$.

- page 577, line -7 should have “≥” instead of “≤.” In any case, the only result we rely on is that when the $\{E_i\}_{i=1}^n$ are disjoint events with $Pr[\bigvee_{i=1}^n E_i] = 1$, then for any event $F$ we have
  \[
  Pr[F] = \sum_{i=1}^n Pr[F \land E_i] = \sum_{i=1}^n Pr[F | E_i] \cdot Pr[E_i].
  \]

- page 578, line 17: $X_i$ should be $X_1$ and $X_j$ should be $X_2$.

- page 594: Algorithm B.13 is missing “if $b > 0$” on the second-to-last line of the algorithm. In line 13 on the page, the number of modular squarings should be $\|b\| - 1$, not $\|b\|$.

Thanks to Claude Crépeau, Bruno Grenet, and Dominique Schröder for informing us about some of the above typos.